International Journal of Communication 11(2017), 763–781 1932–8036/20170005

The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks

LINA DENCIK
JONATHAN CABLE
Cardiff University, UK

The Snowden leaks provided unprecedented insights into the workings of state-corporate surveillance programs based on the interception and collection of online activity. They illustrated the extent of "bulk" data collection and the general and widespread monitoring of everyday communication platforms used by ordinary citizens. Yet public response in the United Kingdom and elsewhere has been considerably muted, and there has been little evidence of public outcry, with often conflicting and inconsistent opinions on the subject. Based on research carried out for the project Digital Citizenship and Surveillance Society, this article explores the nuances of public attitudes toward surveillance, including such attitudes among politically active citizens, through focus groups and interviews. We argue that the lack of transparency, knowledge, and control over what happens to personal data online has led to feelings of widespread resignation, not consent, to the status quo that speaks to a condition we identify as "surveillance realism." We understand this to entail a simultaneous unease among citizens with data collection alongside the active normalization of surveillance that limits the possibilities of enacting modes of citizenship and of imagining alternatives.

Keywords: Snowden, surveillance, activism, public opinion, surveillance realism

The Snowden leaks, first published in June 2013, revealed the extent and scale of digital surveillance and signified an important moment for exploring public understanding and attitudes toward surveillance-related issues. The leaks provided unprecedented insights into the workings of state-corporate surveillance programs based on the interception of Internet traffic and "bulk" collection and analysis of metadata by security agencies in Western democracies, most notably the U.S. National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ). Of particular significance, the Snowden leaks revealed not just instances of business and political espionage or forms of targeted surveillance of particular actors, but rather the general and widespread monitoring of everyday communication among normal citizens. Details of programs such as NSA's PRISM and GCHQ's Tempora outlined in the leaks illustrated the indiscriminate nature of data collection and data storage, leading to the widespread description of the system as one of "mass surveillance" (Bowcott, 2014).

Lina Dencik: dencikl@cardiff.ac.uk
Jonathan Cable: CableJ1@cardiff.ac.uk
Date submitted: 2016–02–29

Discussions of the implications of such surveillance practices for citizens and society have been prevalent (see Isin & Ruppert, 2015; Lyon, 2015). One concern, also expressed by Snowden himself, has been the extent to which such levels of surveillance can create a chilling effect, in which people come to self-police and self-regulate their online communication and behavior (Reitman, 2014). For example, studies carried out post-Snowden have shown a reluctance among citizens to engage with politically sensitive topics online, such as a decline in "privacy-sensitive" search terms on Google (Marthews & Tucker, 2015), a decline in page views of Wikipedia articles relating to terrorism (Penney, 2016), and a "spiral of silence" in surveillance debates on social media (Hampton et al., 2014). The PEN American Center (2013) found evidence of writers' self-censorship in the immediate aftermath of the Snowden leaks. More generally, questions about the entrenched nature of surveillance as an embedded aspect of our everyday communication infrastructure speak to the complex ways in which citizens themselves are entangled in the web of these systems, limiting potential for both circumventing and overcoming them. As journalist Glenn Greenwald (2014) has argued, this comes to have consequences for the possibilities of resistance and social change more broadly:

> Merely organizing movements of dissent becomes difficult when the government is watching everything people are doing. But mass surveillance kills dissent in a deeper and more important place as well: in the mind, where the individual trains him- or herself to think only in line with what is expected and demanded. (pp. 177–178)

Yet public response to the Snowden leaks has varied across countries. Although there have been public displays of dissatisfaction in places such as the "Stop Watching Us" demonstrations in the United States and the "Freedom Not Fear" protests in Germany, the response in the United Kingdom has arguably been considerably more muted, despite the prominent role the UK government was revealed to have in the documents Snowden leaked. It is important to explore such reactions in context and to consider the nuances of public attitudes toward surveillance and such attitudes among otherwise politically active citizens. Based on research carried out for the project Digital Citizenship and Surveillance Society: UK State-Media-Citizen Relations after the Snowden Leaks,[1] this article explores responses to the Snowden leaks among wider society in two respects: (a) the nature of public knowledge of and attitudes toward digital surveillance based on focus group research, and (b) responses to the Snowden leaks among political activists based on semistructured interviews. In particular, the article examines knowledge and awareness of digital surveillance in the aftermath of the Snowden leaks and prominent concerns and reactions.

The United Kingdom provides some interesting insights into the broader social implications of widespread and entrenched systems of surveillance. In this article, we situate findings from our research within the context of what we refer to as *surveillance realism*. This notion draws from the concept of "capitalist realism" advanced by Mark Fisher (2009) to describe the perception of capitalism as the only viable political-economic system, despite widespread recognition of its fallacies and injustices. We use this idea of realism to provide a framework for understanding attitudes to surveillance in the aftermath of Snowden, in which we identify the simultaneous unease and concern with widespread data collection

[1] This project was funded by the UK Economic and Social Research Council.

alongside active normalization and justification of surveillance practices that also come to limit the possibilities for imagining alternative ways of organizing society. This speaks to both a pragmatic response (Hargittai & Marwick, 2016) and a "social imaginary" of resignation (Turow, McGuigan, & Maris, 2015) that prevails in the everyday negotiation with mass surveillance practices, and we situate these in the context of a perceived lack of alternatives.

Surveillance Society After Snowden

To understand the social reactions and responses to revelations of mass surveillance, it is important to situate the publication of the Snowden leaks in the dual context of increasingly security-oriented state conduct in a perceived threat environment and rapidly developing technological capacity to monitor and track human behavior. As Lyon (2015) has argued, surveillance culture came prominently into view simultaneously with intensified security surveillance following 9/11 and the war on terror. In particular, the uncertainty of the form and nature of potential threats in such a political climate provides an apparent necessity and justification for limitless measures to be taken to ward off any such possible threats. Focus, therefore, turns to operationalizing ways of perceiving these potential dangers, with apparatuses of surveillance playing an integral role (Massumi, 2015). In such circumstances, the rise of the "surveillance society" marks a social context characterized by increasing surveillance alongside an explosion in the possible methods and means for observing and monitoring people's behaviors (Lyon, 2001). This is not to suggest that the notion of a surveillance society is something novel (see Lyon, 1994; Rule, 1973), but that contemporary forms of surveillance are intimately linked to securitization and preemption alongside a deeply entrenched technological capacity.

Indeed, a significant aspect of the Snowden leaks in the context of continuous security surveillance is the emphasis on the technological ecology of the surveillance apparatus highlighted in the documents, rooted as it is in the everyday communication infrastructures and platforms of ordinary citizens. Not necessarily new, but publicly evidenced with the Snowden leaks, these practices of surveillance center on an economy that relies on the generation of big data for commercial profit through technologies such as social media platforms. Such operations in turn render ordinary lives increasingly transparent to large organizations, whereas such organizations are increasingly invisible to those whose data are garnered and used (i.e., citizens; Lyon, 2015). In this "data mine" (Andrejevic, 2012) of everyday communication technologies, the users themselves (voluntarily) generate the data that are processed by commercial intermediaries and analyzed by both data brokers and state agencies, highlighting the "participatory" nature of contemporary surveillance (Trottier, 2015). Such a surveillance framework implicates the public in complex ways that speak not only to the entrenchment of surveillance into everyday practices but also to the embedded nature of citizens' lives and relations within the very sustenance of the apparatuses of surveillance-based state–corporate conduct. Harcourt (2015) has also referred to as the "expository society" in which surveillance technology has become woven into the very fabric of our pleasures and fantasies in a society of exposure and exhibition.

Yet despite, or perhaps because of, this intricate web of surveillance and everyday life, as brought to light by the Snowden leaks, citizen knowledge and attitudes to surveillance remain differentiated and convoluted. Opinion polls have repeatedly highlighted the contradictory nature of public

responses to surveillance practices (Harper, Tucker, & Ellis, 2013; see also the compilation of post-Snowden UK opinion polls in Cable, 2015). These can indicate particular trends or tendencies, but surveys and opinion polls provide only a limited picture that is arguably unable to analyze the variability and to capture the complexity in public experiences of surveillance technologies and practices, and more qualitative approaches are needed (Harper et al., 2013). This is not least the case as the context in which people are asked to express opinions about surveillance is defined by a widespread opacity with regard to the actual operation of surveillance, the nature and depth of its penetration, and the protocols in place to act on it (Lyon, Haggerty, & Ball, 2012). Moreover, as Wood and Webster (2009) have argued, referring particularly to the United Kingdom, the contemporary condition of surveillance is one of increasing normalization of surveillance technologies as part of the experience of everyday life as surveillance comes to colonize the domains of emotion, symbolism, and culture:

> The normalization of surveillance is therefore also about far more than just the proliferation of a range of surveillance artefacts and technologies; it is about how these are embedded in the norms and institutions of society and how they are reflective of other aspects of modern society. (p. 264)

Such a Foucauldian understanding of normalization, in which norms of conduct are enforced through discursive practices and institutional sanctions (see also Wahl-Jorgensen & Bennett, 2017) as an exertion of social control, is an important theme in contemporary data-driven surveillance. As Turow, McGuigan, and Maris (2015) outline in their study of customer surveillance in retail spaces, technology companies are

> building a new social imaginary for shopping that reshapes the role of the customer, the nature of the store, and the makeup of the deal so they revolve around the extraction and implementation of huge amounts of data about the individual moving through the retail environment. (p. 470)

Drawing on the work of Charles Taylor and Gramsci's notion of hegemony, Turow et al. (2015) argue that through everyday practices within the retail space as dictated by its increasingly digital architecture and infrastructure, consumers are being institutionalized into taken-for-granted values, habits, and expectations of an increasingly data-driven and discriminatory marketplace. As Taylor (2004) has highlighted in his work on the social imaginary, society and its moral orders are constituted by certain self-understandings in which ordinary people imagine their social surroundings in particular ways that are inducted into common practices and a widely shared sense of legitimacy.

Importantly, social imaginaries are also partly defined by what is commonly perceived as possible. That is, the taken-for-granted understanding of how the everyday world works relies to some extent on the elimination (or at least marginalization) of perceived legitimate alternatives. In his work on explaining the continued prevalence of capitalism, Fisher (2009) refers to this as a form of "realism" in society where a "pervasive atmosphere" conditions culture and regulates work and education. Writing in the wake of the financial crisis, Fisher identifies a "widespread sense that not only is capitalism the only viable political and economic system, but also that it is now impossible even to *imagine* a coherent

alternative to it" (p. 2; italics in original). In this sense, the limits on imagination are a significant aspect of accepting particular systems and infrastructures, despite significant fallacies and injustices. In recent studies on public attitudes to digital surveillance, frequent themes include a general sense of "lack of control" over how information is collected (Eurobarometer, 2015), "privacy fatigue" and prominent confusion about the data-driven systems in place (Hargittai & Marwick, 2016), and a widespread public resignation to the status quo (Turow, Hennesy, & Draper, 2015). This speaks to the restricted environment in which contemporary forms of surveillance through ubiquitous data collection can be challenged in public imagination.

Method

To illustrate how citizens are implicated in systems of surveillance, this article draws on research into responses to the Snowden leaks within the United Kingdom based on qualitative methods examining two aspects of public experiences. We carried out focus groups with various demographics across the United Kingdom from February to August 2015. Our sample consisted of 10 focus groups with 3 to 8 people in each group, emphasizing ethnic, socioeconomic, and geographic diversity (see Table 1). Importantly, these groups' demographics are not statistically representative in any sense; rather, they collectively represent a cross-section of society. In this respect, their categories are not entirely mutually exclusive. As Kitzinger and Barbour (1999) put it, focus groups "encompass diversity and compose a structure" (p. 7) that has been guided by the research questions. However, we have deliberately organized the focus groups to allow us to consider the nuances of diversity with regard to understandings, attitudes, and experiences (Kitzinger, 1994).

Table 1. Sample for Focus Groups.

Group	Demographic	Region	No. of participants
A	Student; age 19–21	Cardiff	5
B	Middle income; 26–45	Treorchy	4
C	Middle income; age 28–52	Plymouth	5
D	High income; age 26–41	London	7
E	Low income; age 32–81	Cardiff	5
F	Retired; age 54–74	Manchester	8
G	South Asian; age 33–39	London	3
H	African Caribbean; age 18–40	Bristol	3
I	Muslim female; age 18–23	Cardiff	5
J	Muslim male; age 18–24	Cardiff	7

Our focus groups lasted 90 minutes on average and engaged with the following themes: (a) understanding and experience of surveillance, (b) knowledge and opinions of the Snowden leaks, (c) attitudes toward intelligence agencies, (d) concerns with privacy and personal data, and (e) online behavior and practices. To ensure that we avoided a self-selecting sample, we did not inform focus group participants beforehand about the subject of the discussion beyond the broad area of digital media. This was a conscious choice to prevent people feeling like they needed prior knowledge to take part. In addition, because of the potential for low levels of knowledge after the first two themes were covered, we

provided participants with an overview of the events of and contexts around the Snowden revelations based on a summary from BBC News Online (2014).[2] We used the same discussion guide, based on 24 questions relating to the various themes, for each group. A semistructured approach allowed the groups to guide the order of questions and to discuss among themselves, and pointed questions catered to all participants. After the focus groups were completed, the material was transcribed and the transcripts fed into the qualitative software NVivo. Themes were then coded based on opinions relating to the key issues to be consistently compared and contrasted across the sample.

Next, we carried out semistructured interviews with a range of political activists, from both big NGOs and smaller community and grassroots organizations based in the United Kingdom. Importantly, to get insight into responses from active citizens more generally, we sought to include groups that were not specifically engaged with digital rights or technology activism and individuals within those groups who were not specifically responsible for technical infrastructures of communication. Our sample, therefore, comprised groups and activists chosen predominantly out of an existing network of contacts that spoke to various social justice concerns with a more or less adversarial relationship to the state. These included environmental activists, labor activists, economic justice activists, antiwar activists, and community and civil liberties groups. The sample consisted of 11 interviews (see Table 2) lasting 60 minutes on average and carried out in person (8) or on Skype (3) from March to June 2015. Similar to the focus groups, our interviews were based on 24 questions and focused on the following themes: (a) understanding and experience of surveillance, (b) knowledge and opinions of the Snowden leaks, (c) attitudes toward state surveillance, (d) online behavior and practices, and (e) changes and other responses to the Snowden leaks. The interviews were semistructured, allowing for flexibility in the conduct of the interviews and the order of questions. The interviews were then transcribed, and NVivo was used to uncover key themes across the sample.

Table 2. Sample for Interviews.

Organization	Orientation
Global Justice Now (GJN)	Economic justice
Campaign Against Arms Trade (CAAT)	Antiarms
CAGE	Rights of victims of the War on Terror
Muslim Association of Britain (MAB)	Community integration
Greenpeace	Environmentalism
Stop the War Coalition (SWC)	Antiwar
Muslim Council of Wales (MCW)	Community integration
Trade Union Congress (TUC)	Workers' rights
Antifracking activist	Environmentalism
ACORN	Community organizing
People's Assembly Against Austerity (PAAA)	Antiausterity

[2] We used the description provided on the BBC website as of January 17, 2014.

We draw from both of these data sets to examine the extent to which we can identify common themes relating to knowledge and understandings of digital surveillance in the aftermath of the Snowden leaks across members of the public, including people who are explicitly politically active. What follows is an overview of first results from the focus groups with the general public and then the interviews with activists, focusing particularly on common themes regarding understandings, knowledge, and concerns about digital surveillance and perceived possibilities for acting on those concerns.

Public Understanding of Surveillance and the Snowden Leaks

The inconsistencies and contradictions that have been evidenced in public opinion polls are a significant feature of people's attitudes and understandings of issues relating to surveillance. Shaped by uncertainty, lack of knowledge, and confusion in many instances, the discussions within our focus groups were frequently marked by still-unformed opinions and attitudes to issues relating to the Snowden leaks and surveillance more broadly. Ascertaining public opinion on these developments therefore requires a cautious approach that recognizes variation and inconsistency in how people think about and express themselves on these matters. In analyzing our focus group discussions, we have sought to outline key themes that we found to be prevalent, explore some of the underlying reasons behind people's inconsistencies, and highlight important areas where we saw significant variation among the demographic groups. We begin by outlining prominent understandings of surveillance before discussing knowledge and attitudes regarding the Snowden leaks and then go on to consider concerns and responses to surveillance practices.

Although our focus group research found variation in how people understand the meaning of surveillance, there was widespread recognition that it is related to forms of "monitoring," "tracking," and being "watched." Often this would be exemplified by apparatuses of surveillance that are closely associated with watching, such as CCTV cameras, which were prominent in people's understandings of what constitutes surveillance. Surveillance was associated with something negative that indicated an activity that takes place without permission or awareness, although some individuals also associated surveillance with notions of "security" and "order." Digital forms of surveillance were less salient in people's initial understandings of surveillance, and issues of data collection did not feature prominently without prompting. However, in steered discussions of metadata in the context of what the United Kingdom's intelligence oversight committee has referred to as "bulk data collection" rather than mass surveillance (Intelligence and Security Committee of Parliament, 2015), our focus group research indicates that people do consider the collection of such data to be surveillance. The concept of metadata itself was not widely known or understood, but when examples of geodata or location data were provided, there was a general consensus that the collection of such data constitutes surveillance:

> Male Speaker (MS)1: If you are able to collect data and see what websites et cetera or if they wanted to go on your e-mail and see who you sent messages to et cetera, you are encountering surveillance. They're watching you.
> MS2: Not just that, they know your location, they know where you live, or they know roughly where you are round and about.
> MS4: Yeah, and what you are doing at all time. (Focus Group J)

> Female Speaker (FS)3: It is still your behavior being tracked, so it is still surveillance in my eyes.
> FS4: Yes, and patterns can be detected; if you're only sending a message to a specific person, they can almost interpret that to be something more than the simple data that they have, so it would be surveillance if they have access to that. (Focus Group I)

Concerns about the collection of such data and the practice of this kind of surveillance were prevalent in most of our focus groups. However, it is important to note that discussions of digital surveillance frequently shifted among actors—sometimes government, sometimes corporations, sometimes employers, sometimes peers—and isolating attitudes toward surveillance as practiced by a particular actor is difficult. This speaks to the ways in which people experience surveillance and how they relate their concerns about surveillance to tangible (or observable) outcomes. The targeted advertising that results from corporate surveillance, for example, was therefore more clearly understood, and concerns about these kinds of practices more coherently expressed, particularly concerning "permission" and who can access the data. Translating these concerns with (meta)data collection to other forms of surveillance, particularly state surveillance as the focus of the Snowden leaks and the concern of this study, is not straightforward. Our research found a general unease with, but much less knowledge about, this form of surveillance, with more ambivalent opinions expressed:

> FS3: I think as soon as it's somebody using your data for a commercial purpose, or if it's the government for I don't know what purpose, but I think that yes, it is part of [surveillance]. I don't like it, I just don't like it. I don't know if it's necessarily surveillance as the terminology . . .
> FS4: It's just that we're not asked if they can, if anybody can use it in any way, because we're not aware of half the things that could be done with it as well. So that's why I think we're talking about work because that's what we can relate to as well, whereas what the government can do with such data I have no idea. I've seen movies like everybody else, but that's about it. (Focus Group C)

> FS1: I think we shouldn't have to be skeptical or wary about what we're doing online or on our phones and stuff, but at the same time it's that element of why? Like, is it such a problem that people are tracking what we're doing that we need to know about it? In the long run they could find out worthwhile things that are not going to ever affect us or harm us. I don't know. (Focus Group A)

These sentiments speak to a general uncertainty about the workings of the system, the purpose of it, and internal negotiations about the benefits and harms of mass surveillance that emerged again and again in discussions across our focus groups. Importantly, our research found that the Snowden leaks and the discussions that have followed have not significantly clarified or enhanced understandings of why and how state surveillance is practiced. Generally, we found low knowledge of both Edward Snowden as a person and of the content of the Snowden leaks. In several instances there was also significant confusion between Snowden and Chelsea Manning, Julian Assange, and WikiLeaks, illustrating how events relating to

whistle-blowing and security become intertwined in public knowledge, as exemplified by the following exchange:

> FS1: A whistle-blower, that's literally all I know.
> MODERATOR: Anyone else?
> MS1: He revealed a lot of U.S. documents from the CIA and I think he's in some embassy, went to Russia, and I think he went to Sweden after.
> MOD: Can you remember any of the content of those documents?
> MS1: A lot of confidential stuff between countries, private information, just damaging to the U.S. government and other governments.
> MS2: But he's in jail for other people's crimes, basically, he's doing the time for people who didn't [expose] depleted uranium use and things? I can't remember.
> MS1: Are you getting mixed up with the other guy with Welsh connections? He's in prison, isn't he?
> MS2: Which one's that?
> MS1: He had connections with West Wales, is it Bradley?
> MS2: I know the one, yes.
> MS1: That's the surname.
> MS2: Yes, I can't remember anything, just that he exposed stuff.
> MS1: I know he revealed a lot of information about what the U.S. government thought about other countries, politicians, and leaders.
> FS1: And they were keeping track of people's communications and stuff in America, I think. (Focus Group B)

However, upon discussion, notions of Snowden being a whistle-blower, working for the American government in some capacity, being in Russia, and having leaked important documents did emerge, although knowledge about the actual content of the leaks was relatively low across the focus groups. When groups were provided a summary, positive opinions about Snowden's leaking the documents were common, with participants describing this as "brave," although there were questions about his motives, whether he had raised his grievances to the proper channels first, the extent to which he may have endangered people, and the added concerns with blowing the whistle on matters of national security as opposed to other matters (e.g., within the public sector) for which whistle-blowers receive less attention. Overall, however, most focus group participants thought that the documents were in the public interest and raised awareness about something important.

Despite participants' recognizing the importance of the leaks, we see a more differentiated picture with regard to the implications of these revelations. Although some expressed "shock" and feelings of being "uncomfortable" or "uneasy" with the subject, particularly with "what little knowledge you have of your own privacy," participants simultaneously expressed a widespread notion that this form of surveillance is justified in certain respects. In particular, mentions of combating terrorism and criminal activity provided a familiar rationale for such practices:

> FS4: I think the government has got to be on their toes because if anything kicks off and there's naught done about it, bloody hell will break loose. (Focus Group F)

> MS2: With a crime or something when, say, an obvious crime is being contemplated or being talked about and that kind of thing, they should intervene, maybe not go away straight ahead and look at it, but just keep an eye on it and make sure that it doesn't snowball into something bigger. . . .
> MS2: Terrorism definitely, that's a big one. (Focus Group A)

However, at the same time, we also found prominent concerns particularly with implications for privacy and questions of the extent of surveillance with notions that "it's been taken too far" and that monitoring does not "need" to be done "in such a permanent manner." Whereas these sentiments stretched across several focus groups, we also found different understandings of these issues among different demographics. For example, in our discussions with young Muslims, the broader political context of these practices was raised as a particular worry:

> FS3: I think if they used it properly, the government, if they used it for surveillance then fine, but I don't think anyone can deny that they're targeting the Muslims. To me it's quite obvious, you can tell that Muslims are being watched more than others and I just think it's gone too far. (Focus Group I)

Such critical perspectives also indicate different experiences of surveillance, with some focus groups having a more prominent awareness of state surveillance. Particularly, those groups who mentioned personal experiences of state surveillance through acquaintances or within the community or who felt they might somehow draw more attention, as in the case of several of our focus groups with ethnic minorities, expressed more explicit concerns with the nature and implications of digital surveillance programs.

Awareness or concerns, however, do not necessarily translate into active resistance or changes in online uses, even among those who have very critical attitudes toward these developments. For example, with regard to using tools that might circumvent digital surveillance, such as encryption and anonymization software such as PGP and Tor, some participants mentioned vague awareness, but little, if any, uptake. Predominantly, the reasoning for this was framed by questions of convenience and a perceived lack of technical ability and knowledge of how to use such tools across age groups, that "it's probably over the top for most people." In some instances such practices were also linked to notions that encryption is about "hiding" something or that it's for people who are "up to something" (Focus Group F).

Rather, proactive responses to surveillance such as using encryption or engaging in protest or critical debate on the topic dissolve within a broader expectation and normalization of various forms of surveillance in everyday life. Although some people said they would make use of alternative technologies if they knew and understood them better, a more prominent theme across all our focus groups was rather a sense of the ubiquity of surveillance, with feelings of a lack of control over what happens to people's information and data and of little power to challenge or change these developments:

> MS2: I guess it is just the age we live in, you know. It's just going to happen. Get used to it, I guess. (Focus Group J)
>
> FS2: I think because so much of what we do is capable of being collected now, I think we've gone beyond that point [of resisting surveillance]. Like, every phone call that you make, every journey that you do on your Oyster, every time that you use the bank card—there's so much out there that's already being tracked, it's just what it will be used for now which is the issue. (Focus Group G)
>
> MS5: For me, I think living in a city we're used to being watched and recorded and you don't even think about it. How many times do you walk past cameras and just not even notice them? (Focus Group D)

As such, surveillance becomes normalized as an everyday occurrence in which it becomes difficult to perceive of ways to actively overcome or circumvent a system of permanent data collection. Instead, as a way of negotiating this "reality" of ubiquitous surveillance, people expressed moments or aspects of self-regulation or attempts to limit access to their data and information through platform settings:

> FS1: I make sure I don't say certain things on Twitter that could possibly make me libelous or something . . . and on Facebook, I make sure everything's private and I do as much private settings on Facebook as possible. Even though I know on the other end, it might not necessarily be as private, but I want it to be as private as I can make it. (Focus Group H)
>
> FS4: I do think about it sometimes like when ISIS was on the news quite a lot, I was scared to Google ISIS because obviously with my background as well, they could interpret that into everything, that I'm going off to Syria because I Googled ISIS . . .
> FS3: Yes, I do think about it, but not all the time. If I'm talking on the phone I know there are certain things that I shouldn't say on the phone because if they're listening, even though I don't mean anything. (Focus Group I)

As these remarks illustrate, our focus group research indicates significant ambivalence among the British public regarding the implications of the Snowden leaks and the realities of mass surveillance more generally. Although it is difficult to isolate state surveillance in people's attitudes and their experiences of living in a surveillance society, these types of practices feed into a general sense of lack of knowledge, understanding, and control over what happens to their data online, by whom, and for what purpose. At the same time, worries about privacy and the extent of (state) surveillance do not translate into active resistance or outcry about these developments. Rather, we see a kind of resignation to the overpowering nature of contemporary surveillance deeply embedded in everyday life and predominantly justified in terms of terrorism and crime. Concerns and unease with (the perceived inevitability of) surveillance in this context comes to be negotiated through varying degrees of caution and self-regulation and attempts to maintain some control over online activity and personal data, but within recognized limited parameters.

Activist Responses to the Snowden Leaks

Although we might assume a more vocal response from our interviews with political activists in the United Kingdom, both the normalization and the sense of resignation to the realities of mass surveillance are also themes that continue within these groups. This is significant, as it illustrates how attitudes to surveillance might incorporate limitations to dissent and the articulation of alternatives. The awareness of state surveillance is relatively entrenched in activist circles in the UK, predominantly because of a particularly troublesome history of police infiltration into activist groups that has marked activist understandings of surveillance and their relationship to the state (Ramsay, Ramsay, & Marsden, 2016). This form of surveillance was also the most prominent description of the meaning of surveillance in our interviews, often with reference to either personal experience or familiarity with others' experiences of such activity, along with CCTV and police presence at demonstrations and actions. Digital surveillance of the kind revealed in the Snowden leaks featured less prominently, but activists recognized that surveillance practices have become increasingly extensive with technological developments: "In the modern context [surveillance] is a hugely expanded field because of the prevalence of the state's ability to intercept social media activity, online activity, as well as the other things that they were always able to intercept" (PAAA activist).

Still, most activists lacked in-depth knowledge of the Snowden leaks and, again, some confused Snowden with WikiLeaks and Chelsea Manning. However, importantly, our interviews indicated a general lack of surprise with revelations of mass surveillance and a widespread expectation that these forms of state practices are being carried out, which is often confirmed to activists when police are present at events they have organized or their activities are intercepted: "It doesn't surprise you; it is exactly what I would expect . . . I think it is scary and it is a really bad and sad state of affairs that I do expect that nothing is private" (ACORN activist). "I think the level of it is terrifying and the more you look into it, the more terrifying it is, but actually I think I probably wasn't surprised" (Antifracking activist).

The internalized expectation of surveillance also means that these revelations were not seen as transformative in and of themselves, but rather that they feed into a consciousness of surveillance that has developed over time:

> I don't think, in fact, that Snowden in particular has had an impact on a single aspect of how we work. . . . In a sense he confirmed what was the sort of thing people suspected was happening anyway, but I don't think that revelation has changed anything we do. (CAAT activist)

In this sense, surveillance is seen as a long-standing, commonplace state practice that has evolved over time. It is a practice that many activists are critical of, particularly when they describe what they view as excessive and intrusive state powers:

> What used to constitute surveillance is protection to real dangers, but now it is more about power to control and protect interests, whether those are interests of big

> corporations, politicians, or "the establishment" and so forth. It is about knowing how to control and label citizens more than helping to positively build society. (CAGE activist)

> When our lives are obstructed in that our e-mails are checked and the basics of investigative journalism are not allowed for "security reasons" and concerns about "terrorism," that is when surveillance becomes exaggerated and the line between "privacy" and "national security" is blurred. (MAB activist)

As such, we find a critical perspective among our interviewees that is simultaneously muted by widespread prior expectation of mass surveillance. This is supported by a perception that the state has insurmountable capabilities to monitor the activities of activists if they wish to do so. In other words, we find that the asymmetrical power dynamic that frequently marks state-activist surveillance relations (Leistert, 2012) is entrenched in the way that many of the activists we spoke with perceive of the contemporary condition. As an MCW activist put it, "Nothing is private anymore," and as a PAAA activist said, "I assume that if the state wants to find out something that we are doing, it will find it out." These kinds of assumptions and perceptions are important because they speak to the general sense of disempowerment that we see as a central aspect of surveillance realism. This is not to say that activists do not think these state powers should be pushed back (they express so clearly), but rather that doing so comes to appear overwhelming. We see this manifest itself in significant ways that illustrate the complex dynamic between surveillance and the possibilities for expressing dissent.

For example, mentions of prioritizing face-to-face interaction, avoiding or regulating online communication about certain types of activities, and maintaining spaces free from technical artifacts all form part of activist communication practices to a greater or lesser extent. These are ways in which activists negotiate living in a surveillance climate while trying to maintain trust and ways of pursuing their agendas. However, another form of negotiation also emerged in our interviews that speaks perhaps more closely to the concerns of a chilling effect. We found that activists evaluate the need to actively be concerned with surveillance and negotiate this through their agendas, relations to the state, and how radical their politics are. In other words, some interviews indicated that surveillance only becomes a concern for activists if they feel that their activities fall outside an acceptable mainstream framework. Many of them perceive themselves (and perhaps even strive) to fall safely within such a framework:

> I think we are a pretty transparent organization. I think by in large anything we are working on usually goes public a few days later. Whether that is in the various media or updates to our website. I don't think we have a huge amount to hide, but even in terms of our finances, we obviously don't make those public. But equally, I'm also well aware that if the state ever really wanted to get their hands on them they could probably, or already have. We don't see that as being a particular concern. (CAAT activist)

> The truth is that we've got nothing to hide, we're against government on these issues, we're mobilizing against them, we're not breaking any laws. (SWC activist)

Of course, such a position cannot be divorced from the broader political climate in which, for example, the activists from Muslim community groups and advocates of civil rights for Muslims expressed a heightened consciousness of the ways in which their agendas, activities, and communications could be seen as more challenging to the mainstream or could be "misconstrued":

> I'm wary, particularly with this cloud and everything. With my mobile phone, there's no point in worrying about it because everybody knows everything anyway. So you just have to make sure that you don't do anything which could be misconstrued—that's how I see it and that's what I advise to people. (MCW activist)

Ubiquitous surveillance, in this regard, and the feeling of profound asymmetry in power relations can be seen as a (self-)regulatory environment in which activists come to negotiate the costs and benefits of more radical politics, whatever the current political climate might dictate such to be, arguably keeping the mainstream in check. It manifests itself as a "pervasive atmosphere" that constrains thought and action, to use the terms of Mark Fisher (2009). The use of encryption tools in such a context was described as a shift to "hidden" and "closed" practices that contradict activist pursuits of transparency and inclusivity, echoing sentiments of the familiar "nothing to hide, nothing to fear" rationale (see also Mols, forthcoming):

> We would [use encryption] if we felt there was a reason to do it. We are aware of it, it is just we haven't seen any evidence of something that is particularly problematic that we need to do. (TUC activist)

> In terms of encrypting software and things, we don't use it with ACORN. I've stopped doing a lot of that just because I think a more open, a more accessible approach within community organizations is just more effective than small groups applying pressure tactics. (ACORN activist)

Such sentiments indicate that circumventing surveillance through technological means is seen to be at odds with inclusivity and transparency. This stems partly from a perception that these practices, and privacy activism more broadly, require expert knowledge and skills:

> At the moment, it's terribly in favor of state surveillance, in favor of lack of privacy, and I think something needs to be done to redress that balance, which is probably action by individuals to reassert their privacy. But it feels like there are few routes to doing that at the moment unless you're clued in or know what you're doing. (Greenpeace activist)

In this sense, actively resisting surveillance or engaging with surveillance as an issue is seen as a specialist practice that is confined to technology activists or digital rights groups. Although the activists we interviewed expressed widespread solidarity with the pursuits of these communities when asked, they also expressed a certain disconnection with their concerns and activities and an inability to properly engage with them. In other words, the issue of surveillance is outsourced to these expert communities rather than being an integrated activist concern (see also Dencik, Hintz, & Cable, 2016).

The feeling of disconnection speaks partly to the entrenched dependency on surveillance technologies (e-mail, social media, mobile phones, etc.) that activists use as part of their organizing and campaigning and the feeling that circumventing or resisting these (widely seen as beneficial) technological infrastructures seems too overwhelming and too draining of already scarce resources. Although some activists do navigate around these technologies for particular aspects of their activities (e.g., organizing direct actions), we also see a prominent sense of disempowerment with regard to the ability to keep actual autonomous or private spaces of practice. Instead, negotiation with the realities of surveillance circulates around the reliance on an acceptable (mainstream) framework that forms the parameters for activities and expression. Although explicitly critical of state surveillance in light of the Snowden leaks, participants perceived a lack of resources or avenues to resist it within the context of their agendas and practices, which means that they outsource active concern with surveillance to expert communities, confining it as a specialist issue.

The Advent of Surveillance Realism?

Public debate about the Snowden leaks and digital surveillance has crystallized the ongoing security-centered political climate that has marked post-9/11 societies, not least the United Kingdom. Revelations of mass surveillance have been met with muted responses from large sections of society that do not necessarily constitute consent to these activities, but rather indicate ambivalence, confusion, and lack of knowledge about not just the operations of digital surveillance but also what can actually be done about them. In such an environment, we find that unease with and worries about surveillance do not necessarily translate into fully formed opinions and active resistance to state practices, but rather that they become negotiated and disregarded with familiar justifications of security and the entrenched nature of surveillance into everyday life that limit alternatives.[3] Within this context, enactments of citizenship, not least political activism, are modified in relation to surveillance in moments in which citizens seek to self-regulate their behavior, position themselves according to what might be uncontroversial, or attempt to control the flow of their data in what is recognized as a limited capacity, without necessarily engaging critically with the system as a whole.

We refer to this contemporary condition as a form of "surveillance realism" (drawing on Fisher's [2009] use of *realism*) in which lack of transparency and knowledge in conjunction with the active normalization of surveillance through discursive practices and institutional sanctions manifested in its ubiquity comes to negate prominent concerns, ultimately limiting possibilities for alternative imaginations of organizing society. Importantly, this notion does not indicate acceptance of or even consent to the prevalence of surveillance technologies, but rather relates to the pragmatism and resignation that has been widely identified in more qualitative research on post-Snowden public attitudes and responses. We see here also a sense of disempowerment that speaks to the feeling of the overwhelming nature of technological capacity to monitor and collect data that also means that circumvention or resistance to surveillance is externalized to those with expert knowledge, skills, and resources. Moreover, identifying or

[3] As we noted earlier, although our study focused particularly on state surveillance, isolating surveillance to a particular actor is difficult, and further research is needed on attitudes toward the role of corporations in surveillance and the turn to data mining by a host of other actors (Kennedy, 2016).

articulating an alternative way of organizing society becomes increasingly difficult as data collection becomes routine and justified. As such, we introduce surveillance realism as a concept that can encompass the entrenched and complex ways in which citizens are implicated in contemporary forms of surveillance through everyday technologies and how they negotiate this. In particular, it speaks to the simultaneous concern with data collection and the perceived inability to do much about it, as identified in our research, that we see lead to the compromised position in which citizens, whether politically active or not, depend on their activities being sufficiently uncontroversial and acceptable that they have nothing to hide and nothing to fear. At the same time, the politically and socially contingent nature of such a position is widely understood, particularly in communities that feel more marginalized and targeted.

The implications of surveillance realism for citizenship as it is increasingly digitally mediated are significant. As we have illustrated in this article, aspects of a chilling effect emerge within the ongoing negotiations of interacting with surveillance technologies in everyday life, both for ordinary communication and for pursuing particular forms of social change or expressing dissent. Also, significantly, the feelings of a lack of knowledge about and a lack of control over digital infrastructures and activities create simultaneous unease and disempowerment. This problematizes the notion of informed consent to state surveillance and undermines democratic legitimacy and accountability. Moreover, it limits the possibilities for enacting aspects of citizenship particularly with regard to not only articulating, but even imagining other ways of organizing society that are more in line with the concerns for privacy and civic rights that are still prominent in how people feel. Surveillance realism, in this regard, serves to narrow the parameters for responses to the Snowden leaks and acts as a "pervasive atmosphere" that comes to "constrain thought and action" (Fisher 2009, p. 16) in line with surveillance society, limiting the possibilities for alternatives.

Conclusion

Opinions on surveillance are difficult to ascertain in consistent and concrete terms, but the confusion and inconsistency stem partly from a lack of transparency and knowledge that has important implications for understandings of citizenship. As our research on public attitudes and activist responses in light of the Snowden leaks shows, a prevalent theme in people's entanglement in the everyday technologies and communication platforms that sustain contemporary forms of digital surveillance is a sense of resignation to a system of ubiquitous data collection, despite prominent concerns and feelings of unease. The normalization of surveillance is negotiated through various pragmatic responses—internalized justification, forms of self-regulation, and the outsourcing of resistance to others—that also depend on the limited perception of what else is possible. We suggest thinking of this as a form of "surveillance realism" that can be further advanced as a framework for highlighting the complex ways in which citizens are embedded in contemporary forms of surveillance that also limits the possibilities for imagining alternative ways of organizing society. This concept, we argue, becomes especially pertinent in discussions on digital citizenship.

References

Andrejevic, M. (2012). Exploitation in the data mine. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance: The challenges of Web 2.0 and social media* (pp. 71–88). New York, NY: Routledge.

BBC News Online. (2014, January 17). Edward Snowden: Leaks that exposed U.S. spy programme. *BBC News*. Retrieved from http://www.bbc.co.uk/news/world-us-canada-23123964

Bowcott, O. (2014, December 8). Mass surveillance exposed by Snowden "not justified by fight against terrorism." *The Guardian*. Retrieved from https://www.theguardian.com/world/2014/dec/08/mass-surveillance-exposed-edward-snowden-not-justified-by-fight-against-terrorism

Cable, J. (2015). *Working paper: An overview of public opinion polls since the Edward Snowden revelations in June 2013*. Cardiff University. Retrieved from http://sites.cardiff.ac.uk/dcssproject/files/2015/08/UK-Public-Opinion-Review-180615.pdf

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambivalence of anti-surveillance resistance in political activism. *Big Data & Society, 3*(2), 1–12. doi:10.1177/2053951716679678

Eurobarometer. (2015). *Data protection* (Special Eurobarometer report 431). Retrieved from http://ec.europa.eu/public_opinion/archives/eb_special_439_420_en.htm

Fisher, M. (2009). *Capitalist realism: Is there no alternative?* Hants, UK: Zero Books.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA and the surveillance state*. London, UK: Hamish Hamilton.

Hampton, K. N., Rainie, L., Lu, W., Dwyer, M., Shin, I., & Purcell, K. (2014). *Social media and the "spiral of silence."* Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/files/2014/08/PI_Social-networks-and-debate_082614.pdf

Harcourt, B. E. (2015). *Exposed: Desire and disobedience in the digital age*. Cambridge, MA: Harvard University Press.

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10,* 3737–3757.

Harper, D., Tucker, I., & Ellis, D. (2013). Surveillance and subjectivity: Everyday experiences of surveillance practices. In K. Ball & L. Snider (Eds.), *The surveillance-industrial complex: A political economy of surveillance* (pp. 175–190). London, UK: Routledge.

Intelligence and Security Committee of Parliament. (2015, March 12). *Privacy and security: A modern and transparent legal framework*. UK House of Commons. Retrieved from https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7cpVcpQ7oNu0pTSkCUaq72BIl7tMqsXIu7GcTKSdWEocZ4QbaCc2IGNdvkTsrXnZmOEOE7VWbbOoxKIgzGDarLhdLAZjwNY5cBlPCFmIhW4pvoCFCnZwH22Jja6AwEwOkKD-ztcDgUiCuCPFoRoESS7lclVXtg2e7BGLmCJiWCBIYM1x0KyVBArb32Q4r_N5uFqOdjICtFB75oQR3j-K_BQMFlYxnhlQGZo8z3Kvb4jqSdgDFh9Yav2W-CImbZn8DFiKnUA-&attredirects=0

Isin, E., & Ruppert, E. (2015). *Becoming digital citizens*. London, UK: Rowman & Littlefield International.

Kennedy, H. (2016). *Social media data mining becomes ordinary*. Basingstoke, UK: Palgrave.

Kitzinger, J. (1994). The methodology of focus groups: The importance of interaction between research participants. *Sociology of Health & Illness, 16*(1), 103–121.

Kitzinger, J., & Barbour, R. S. (1999). Introduction: The challenge and promise of focus groups. In R. S. Barbour & J. Kitzinger (Eds.), *Developing focus group research: Politics, theory and practice* (pp. 1–20) London, UK: SAGE Publications.

Leistert, O. (2012). Resistance against cyber-surveillance within social movements and how surveillance adapts. *Surveillance & Society, 9*(4), 441–456.

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. Cambridge, UK: Polity Press.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Buckingham, UK: Open University Press.

Lyon, D. (2015). *Surveillance after Snowden*. Cambridge, UK: Polity Press.

Lyon, D., Haggerty, K. D., & Ball, K. (2012). Introduction: Understanding surveillance. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 15–18). London, UK: Routledge.

Marthews, A., & Tucker, C. (2015). *Government surveillance and Internet search behaviour*. Social Science Research Network. Retrieved from http://ssrn.com/abstract=2412564

Massumi, B. (2015). *Ontopower: War, powers, and the state of perception*. Durham, NC: Duke University Press.

Mols, A. (Forthcoming). "Not interesting enough to be followed by the NSA": Framing Dutch privacy attitudes in the aftermath of the NSA revelations. *Digital Journalism*.

PEN American Center. (2013). *Chilling effects: NSA surveillance drives U.S. writers to self-censor*. New York, NY: PEN American Center. Retrieved from http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf

Penney, J. (2016). Chilling effects: Online surveillance Wikipedia use. *Berkeley Technology Law Journal, 31*(1), 117. Retrieved from http://ssrn.com/abstract=2769645

Ramsay, G., Ramsay, A., & Marsden, S. (2016, May 24). Report: Impacts of surveillance on contemporary British activism. *openDemocracyUK*. Retrieved from https://www.opendemocracy.net/uk/gilbert-ramsay/report-impacts-of-surveillance-on-contemporary-british-activism

Reitman, R. (2014). Snowden's motivation: What the Internet was like before it was being watched, and how we can get there again [Web log post]. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2014/10/snowden-motivated-what-internet-was-it-was-being-watched-and-how-we-can-get-there

Rule, J. B. (1973). *Private lives and public surveillance*. London, UK: Allen Lane.

Taylor, C. (2004). *Modern social imaginaries*. Durham, NC: Duke University Press.

Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies, 18*(4–5), 530–547.

Turow, J., Hennesy, M., & Draper, N. (2015). *The tradeoff fallacy*. Report from the Annenberg School of Communication, University of Pennsylvania. Retrieved from https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Turow, J., McGuigan, L., & Maris, E. R. (2015). Making data mining a natural part of life: Physical retailing, customer surveillance and the 21st century social imaginary. *European Journal of Cultural Studies*, *18*(4–5), 464–478.

Wahl-Jorgensen, K., & Bennett, L. (2017). The normalization of surveillance and the invisibility of digital citizenship: Media debates after the Snowden revelations. *International Journal of Communication, 11*. Special section on Digital Citizenship and Surveillance.

Wood, D. M., & Webster, C. W. R. (2009). Living in surveillance societies: The normalisation of surveillance in Europe and the threat of Britain's bad example. *Journal of Contemporary European Research, 5*(2), 259–273.